REMARKS

In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application. This amendment is believed to be fully responsive to all issues raised in the July 7, 2006 Office Action.

Substance of Examiner Interview

In an Examiner Interview conducted November 15, 2006, claim 1 was discussed. The Examiner indicated that amending claim 1 to clearly indicate that a first electronic device is responsible for deriving the digital signature and associating the digital signature with a web page, while a second electronic device is responsible for authenticating the digital signature would overcome the 103 rejection of claim 1 based on Bal in view of Cox. The Examiner further suggested amending claim 1 to indicate that the claimed web page does not include the control object, but merely code to invoke a control object.

The Applicant appreciates the Examiner's courtesy and willingness to discuss this matter.

Amendments to the Claims

Claims 1, 3, and 4 are amended to clarify the processing performed by first and second electronic devices.

Rejections to the Claims

35 U.S.C. 103(a)

Claims 1-4, 6, 10, 19, 21, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,499,109 issued to Balasubramaniam et al. (herein referred to as "Bal") in view of U.S. Patent Number 6,253,323 issued to Cox et al. (herein referred to as "Cox").

Applicant's application describes techniques for limiting access to potentially dangerous code. A control object made up of executable code may be downloaded to a client device via a web page. Other web pages may then attempt to execute the control object that was previously downloaded. To ensure that the control object is not invoked maliciously, Applicant's application describes digitally signing a web page that invokes a control object before the web page is delivered to a client computer. Applicant's application also describes authenticating the source of a web page that attempts to invoke the control object, and then verifying that the identified source is authorized to invoke the control object. The authentication is performed based on the digital signature that is associated with a web page that attempts to invoke the control object. The authorization may be performed in any of a number of ways, including, but not limited to, comparing the source of the web page with a list of authorized sources. If either the authentication or the authorization fails, then the control object is not invoked.

Claim 1 has been amended, rendering the rejection of claim 1 moot. However, Applicant believes that claim 1, as amended is allowable over Bal in view of Cox as discussed below.

As amended, claim 1 recites:

> A method, comprising:
>
> A first electronic device deriving a digital signature and associating the digital signature with a web page only if the web page includes code to invoke a control object; and
>
> Subsequent to associating the digital signature with the web page, the first electronic device delivering the web page to a second electronic device capable of authenticating the digital signature such that the second electronic device executes at least a portion of the web page in response to authenticating the digital signature.

The combination of Bal and Cox does not teach or suggest, "a first electronic device deriving a digital signature and associating the digital signature with a web page only if the web page includes code to invoke a control object; and subsequent to associating the digital signature with the web page, the first electronic device delivering the web page to a second electronic device," as recited in claim 1.

Bal describes verifying the source of software downloaded from a remote site to a client computer over a computer network before the software can be executed on the client computer. (Bal, Abstract.) Specifically, Bal describes a

computer-executable program code that first determines the URL to which a browser running on the client computer is pointed and enables the downloaded software program only if the URL to which the browser is pointed is an authorized URL. (Bal, Summary.)

Cox describes multiple embodiments of an object-based digital signature that may allow digital signatures to approve or verify portions of documents, address issues associated with the temporal ordering of digital signatures, and allow information dispersed over a network of computing systems to be verified or approved. (*Cox*, column 6, lines 13-23.) Cox also describes an object based digital signature that allows digital signatures to approve or validate portions of documents. (*Cox*, column 6, lines 55-57.)

Neither Bal nor Cox teach or suggest "a first electronic device deriving a digital signature and associating the digital signature with a web page ***only if*** the web page includes code to invoke a control object; and subsequent to associating the digital signature with the web page, the first electronic device delivering the web page to a second electronic device," as recited in claim 1. The Office cites Bal, column 2, line 43 – column 3, line 19 and column 6, lines 20-29 as teaching "associating an authentication code with a web page only if the web page includes code to invoke a control object." The Office also states that the cited portions of Bal teach checking "whether the web site is authorized web site when the software is invoked by the script." (*Office Action, page 2.*)

Checking whether the web site is an authorized web site when the software is invoked by the script is not the same as authenticating a digital

signature associated with a web page, as claimed. Specifically, the checking whether the web site is an authorized web site, as described in Bal, is performed by the electronic device that receives the web site (e.g., the claimed second electronic device), and not by the electronic device that delivers the web page (e.g., the claimed first electronic device).

Furthermore, the Office states:

> Regarding applicant's remarks, applicant argues that the references do not disclose associating the digital signature with a web page only if the web page includes code to invoke a control object. However, examiner disagrees. Bal reference discloses that the first check takes place when the script is detected and running on client computer to invoke the software (Bal: column 6 lines 22-25). Therefore, applicant's argument is respectfully traversed because associating with a digital signature occurs when the script is detected and running on client computer. (*Office Action, page 5.*)

The Office is contending that the combination of Bal and Cox teaches associating a digital signature with a web page when the script is detected and running on the client computer. This interpretation is inconsistent with the language of claim 1. As stated above, claim 1 recites, "a first electronic device deriving a digital signature and associating the digital signature with a web page...; and subsequent to associating the digital signature with the web page, the first electronic device delivering the web page to a second electronic device capable of authenticating the digital signature such that the second electronic device executes at least a portion of the web page in response to authenticating

the digital signature." The claim language clearly teaches that the digital signature is associated with the web page prior to the web page being delivered to the client computer. Accordingly, the Office's interpretation of Bal that, "associating with a digital signature occurs when the script is detected and running on client computer," does not teach the limitations of claim 1.

Accordingly, for at least these reasons, claim 1 is allowable over Bal in view of Cox.

Claims 2-4, 6, 10, 19, 21, and 22 are allowable by virtue of their direct or indirect dependence on claim 1. Furthermore, one or more of claims 2-4, 6, 10, 19, 21, and 22 may also be allowable over Bal in view of Cox for other reasons.

For example, claim 3 recites, "in an event that the web page does not include code to invoke the control object, the first electronic delivering the web page without a digital signature." Neither Bal nor Cox teach or suggest delivering a web page without a digital signature in an event that the web page does not include code in invoke a control object. Bal does not teach or suggest digitally signing any web pages; and Cox describes a way in which web pages can be digitally signed, but does not suggest signing or not signing a web page based on whether or not the web page includes code to invoke a control object.

With regard to claim 3, the Office cites Bal, column 7, lines 29-51. The Office contends that the cited portion of Bal teaches, "determine that a control object is present in the web page and then authenticate whether the web site is authorized." (*Office Action, page 3.*) The determining and authenticating

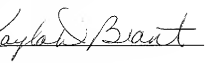
described by the Office is performed by a client computer after receiving the web page, and is not the same as "in an event that the web page does not include code to invoke the control object, the first electronic device delivering the web page without a digital signature," as recited in claim 3. Accordingly, claim 3 is also allowable over Bal in view of Cox.

Conclusion

Claims 1-4, 6, 10, 19, 21, and 22 are believed to be in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the present application. Should any issue remain that prevents immediate issuance of the application, the Examiner is encouraged to contact the undersigned agent to discuss the unresolved issue.

Respectfully Submitted,
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

Dated: 11/20/2006



Name: Kayla D. Brant
Reg. No. 46,576
Phone No. (509) 324-9256 ext. 242